Attorney Docket No. 032326-292

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Jean-Sebastien Coron et al.	Group Art Unit:
Application No.: Unassigned	Examiner:
Filed: January 26, 2005	Confirmation No.:
For: A DATA ENCIPHERING METHOD AND ASSOCIATED CRYPTOGRAPHIC SYSTEM AND COMPONENT (As Amended)	

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

The listed documents were cited in the International Search Report in the corresponding PCT application.

To assist the Examiner, the documents are listed on the attached form PTO-1449. However, copies of the documents are not provided as it is understood that they have already been transmitted by the International Bureau. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date January 26, 2005

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

10/522420

Substitute for form 1449A/PTO & 1449B/PTO

FIRST INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known

DT05 Rec'd PCT/PTO 26 JAN 2005

Application Number	
Filing Date	January 26, 2005
First Named Inventor	Jean-Sebastien Coron et al.
Examiner Name	
Attorney Docket Number	032326-292

U.S. PATENT DOCUMENTS

Examiner Initials	Document Number	Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Issue/Publication Date (MM-DD-YYYY)

FOREIGN PATENT DOCUMENTS

Examiner Initials	Document Number	Kind Code (if known)	Country	Date of Publication (MM-DD-YYYY)	STATUS						
					Translation	Partial Translation	Eng. Lang. Summary	Search Report	IPER	Abstract	Cited in Spec

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	BELLARE M. et al., "The Exact Security of Digital Signatures – How to Sign With RSA and Rabin", Advances in Cryptology – Eurocrypt '96. International Conference on the Theory and Application of Cryptographic Techniques. Saragossa, May 12-16, 1996, pages 399-416 XP000725449 ISBN: 3-540-61186-X.
	BELLARE, M., ROGAWAY, P., "Optimal Asymmetric Encryption – How to Encrypt with RSA", Full version of the paper that appeared in the Proceedings of Advances in Cryptology – Eurocrypt ' 94, 19 November 1995, XP002238170, page 2, line 1 – page 3, line 12.
	HABER, S., PINKAS, B., "Securely Combining Public-Key Cryptosystems", Proceedings of the ACM Computer and Security Conference, November 2001, XP002238171, page 215, left-hand column, line 1 – line 9, page 221, left-hand column, line 58 – right hand column, line 11.
	CORON J.-S. et al., "Universal padding schemes for RSA", Advances in Cryptology – Crypto 2002. 22nd Annual International Cryptology Conference. Proceedings (Lecture notes in Computer Science Vol. 2442), 2002, Berlin, Germany, Springer-Verlag, Germany, pages 226-241, XP002265380, ISBN: 3-540-44050-X.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.